

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-181533

(43)Date of publication of application : 07.07.1998

(51)Int.Cl.

B60R 25/04

B60R 25/00

E05B 49/00

E05B 65/19

E05B 65/20

H04L 9/32

H04Q 9/00

(21)Application number : 08-345908

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 25.12.1996

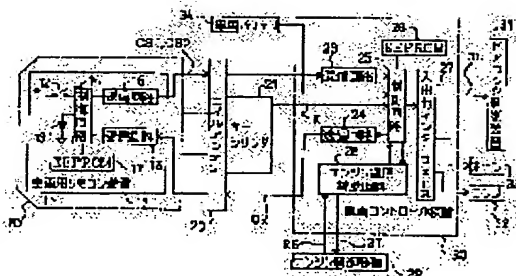
(72)Inventor : HISADA TAKAYUKI  
MIYAZAKI TAKAO  
KATAYAMA KAZUYORI

## (54) REMOTE CONTROL DEVICE FOR VEHICLE AND VEHICLE SECURITY DEVICE

## (57)Abstract:

PROBLEM TO BE SOLVED: To provide a vehicle remote control device which makes a bidirectional communication possible by integrating an immobilizer and keyless entry functions, and carries out cost reduction and maintenance labor reduction by reducing the number of parts.

SOLUTION: A remote control device has a circuit 16 for receiving a cipher source code CR from a vehicle side when a key 10 is inserted into a key cylinder 21; a circuit 17 for storing the cipher source code; a control circuit which creates the first ciphered code CS1 responding to the cipher source code, and creates the second ciphered code CS2 responding to the operation of a manual switch 12; and a transmitting circuit 15 for transmitting each ciphered code toward a vehicle through a radio wave signal. The first ciphered code includes a command for permitting the engine start of the vehicle, and the second ciphered code is created on the ciphered code in a memory circuit and includes a command for locking and unlocking the door lock of the vehicle.



## LEGAL STATUS

[Date of request for examination] 10.02.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3256666

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 10-181533

(43) 公開日 平成10年(1998)7月7日

(51) Int. Cl. <sup>6</sup>	識別記号	F I
B 6 0 R	25/04 6 0 2	B 6 0 R 25/04 6 0 2
	25/00 6 0 5	25/00 6 0 5
E 0 5 B	49/00	E 0 5 B 49/00 K
	65/19	65/19 D
	65/20	65/20
審査請求	未請求	請求項の数 2 0 O L
		(全 2 0 頁) 最終頁に続く

(21) 出願番号 特願平8-345908

(22) 出願日 平成8年(1996)12月25日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 久田 崇之

兵庫県神戸市兵庫区浜山通6丁目1番2号

三菱電機コントロールソフトウェア株式会社  
社内

(72) 発明者 宮崎 孝夫

東京都千代田区丸の内二丁目2番3号 三菱  
電機株式会社内

(72) 発明者 片山 和頼

東京都千代田区丸の内二丁目2番3号 三菱  
電機株式会社内

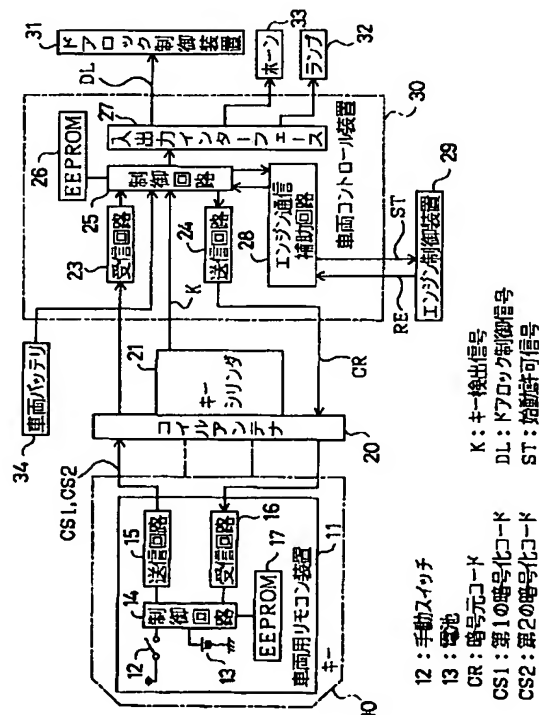
(74) 代理人 弁理士 曾我 道照 (外6名)

(54) 【発明の名称】 車両用リモコン装置および車両セキュリティ装置

(57) 【要約】

【課題】 イモビライザ、キーレスエントリ機能を一体化して双方向通信可能とし、部品削減によりコストダウンおよびメンテナンス労力を低減した車両用リモコン装置を得る。

【解決手段】 キーシリンダ21へのキー10の挿入時に車両側からの暗号元コードCRを受信する回路16と、暗号元コードを記憶する回路17と、暗号元コードに应答して第1の暗号化コードCS1を生成するとともに手動スイッチ12の操作に应答して第2の暗号化コードCS2を生成する制御回路と、各暗号化コードを電波信号により車両側に送信する送信回路15とを備え、第1の暗号化コードは、車両のエンジン始動を許可するための指令を含み、第2の暗号化コードは、記憶回路内の暗号元コードに基づいて生成され、車両のドアロックの施錠または開錠するための指令を含む。



## 【特許請求の範囲】

【請求項 1】 車両のエンジン始動用のキーシリンダに挿入されるキーに内蔵され、且つ前記車両との間で相互に通信を行う車両用リモコン装置であって、前記キーシリンダへの前記キーの挿入時に前記車両側から送信される暗号元コードを受信する受信回路と、前記暗号元コードを記憶する記憶回路と、ユーザにより操作される手動スイッチと、前記暗号元コードの受信にตอบสนองして第 1 の暗号化コードを生成するとともに、前記手動スイッチの操作にตอบสนองして第 2 の暗号化コードを生成する制御回路と、前記第 1 および第 2 の暗号化コードを電波信号により前記車両側に送信する送信回路とを備え、前記第 1 の暗号化コードは、前記車両のエンジン始動を許可するための指令を含み、前記第 2 の暗号化コードは、前記記憶回路内の暗号元コードに基づいて生成され、前記車両のドアロックの施錠または開錠するための指令を含むことを特徴とする車両用リモコン装置。

【請求項 2】 前記暗号元コードは、前記車両を特定するために設定されたトリガ信号を含み、前記制御回路は、前記トリガ信号に基づいて前記暗号元コードの正規を判定するとともに、前記トリガ信号にตอบสนองして前記第 1 の暗号化コードを生成し、前記記憶回路は、正規と判定された前記暗号元コードのみを記憶することを特徴とする請求項 1 に記載の車両用リモコン装置。

【請求項 3】 前記制御回路は、前記記憶回路に記憶された前記暗号元コードに基づいて、通信毎に異なる前記第 2 の暗号化コードを生成することを特徴とする請求項 1 に記載の車両用リモコン装置。

【請求項 4】 前記第 1 および第 2 の暗号化コードは、互いに異なることを特徴とする請求項 1 に記載の車両用リモコン装置。

【請求項 5】 前記第 1 の暗号化コードの電波出力は、前記第 2 の暗号化コードの電波出力よりも小さく設定されたことを特徴とする請求項 1 に記載の車両用リモコン装置。

【請求項 6】 前記暗号元コードは、電波信号からなり、前記受信回路は、インダクタンスを有するコイルとキャパシタンスを有するコンデンサとからなる共振回路を含み、前記共振回路を介した電磁結合により前記暗号元コードを受信することを特徴とする請求項 1 に記載の車両用リモコン装置。

【請求項 7】 前記暗号元コードは、磁気信号からなり、前記受信回路は、磁気抵抗素子を含み、前記磁気抵抗素子を介して前記暗号元コードを受信することを特徴とする請求項 1 に記載の車両用リモコン装置。

【請求項 8】 前記暗号元コードは、磁気信号からなり、

前記受信回路は、ホールセンサを含み、前記ホールセンサを介して前記暗号元コードを受信することを特徴とする請求項 1 に記載の車両用リモコン装置。

【請求項 9】 前記暗号元コードは、光信号からなり、前記受信回路は、受光素子を含み、前記受光素子を介して前記暗号元コードを受信することを特徴とする請求項 1 に記載の車両用リモコン装置。

【請求項 10】 前記暗号元コードは、電波信号からなり、前記受信回路は、高周波受信回路からなることを特徴とする請求項 1 に記載の車両用リモコン装置。

【請求項 11】 前記車両用リモコン装置が内蔵されたキーと、前記車両に設けられて、前記キーの挿入時にキー検出信号を生成するキーシリンダと、前記車両に搭載されて、前記車両用リモコン装置との間で相互に通信を行う車両コントロール装置とを備え、

前記車両コントロール装置は、前記車両用リモコン装置から送信される前記第 1 および第 2 の暗号化コードを受信する受信手段と、前記キー検出信号にตอบสนองして前記暗号元コードを生成するとともに、前記第 1 および第 2 の暗号化コードの受信にตอบสนองして前記車両のエンジンおよびドアを制御する制御手段と、

前記暗号元コードを前記車両用リモコン装置に送信するための送信手段とを含み、前記制御手段は、前記第 1 の暗号化コードにตอบสนองして前記車両のエンジン始動を許可するとともに、前記第 2 の暗号化コードにตอบสนองして前記車両のドアロックを制御することを特徴とする請求項 1 に記載の車両用リモコン装置を用いた車両セキュリティ装置。

【請求項 12】 前記制御手段は、通信毎に異なる前記暗号元コードを生成することを特徴とする請求項 11 に記載の車両セキュリティ装置。

【請求項 13】 前記制御手段は、通信毎にランダムカウンタ値を用いて前記暗号元コードを生成することを特徴とする請求項 12 に記載の車両セキュリティ装置。

【請求項 14】 前記暗号元コードは、前記第 1 の暗号化コードの送信要求を前記車両用リモコン装置に指令するためのトリガ信号を含むことを特徴とする請求項 11 に記載の車両セキュリティ装置。

【請求項 15】 前記トリガ信号は、前記車両を特定するために設定された複数のデータの組み合わせからなることを特徴とする請求項 14 に記載の車両セキュリティ装置。

【請求項 16】 前記車両コントロール装置内の制御手段は、前記第 2 の暗号化コードにตอบสนองして、前記車両のドアロックを制御するとともに、前記車両のエンジン始

動を許可することを特徴とする請求項 11 に記載の車両セキュリティ装置。

【請求項 17】 前記車両用リモコン装置内の制御回路は、前記第 2 の暗号化コードを送信毎に変更し、前記車両コントロール装置内の制御手段は、前記第 2 の暗号化コードを受信毎に変更し、前記車両コントロール装置は、受信毎に変更される前記第 2 の暗号化コードを記憶する記憶手段を含み、前記制御手段は、受信された前記第 2 の暗号化コードと、前記記憶手段に記憶された前記第 2 の暗号化コードとの差が一定範囲以内のときに、受信された前記第 2 の暗号化コードを正規と判定し、正規と判定された前記第 2 の暗号化コードのみに応答して、前記車両のドアロックを制御することを特徴とする請求項 11 に記載の車両セキュリティ装置。

【請求項 18】 前記車両コントロール装置内の送信手段と協動するように前記キーシリンダに配設されたリング状のコイルアンテナを備え、前記車両用リモコン装置内の受信回路は、インダクタンスを有するコイルとキャパシタンスを有するコンデンサとからなる共振回路を含み、前記暗号元コードは、電波信号からなり、前記共振回路を介した電磁結合により、前記コイルアンテナから前記受信回路に送信されることを特徴とする請求項 11 に記載の車両セキュリティ装置。

【請求項 19】 前記車両コントロール装置内の送信手段と協動するように前記キーシリンダに配設された磁石手段を備え、前記暗号元コードは、磁気信号からなり、磁気応答作用により前記磁石手段を介して前記車両用リモコン装置内の受信回路に送信されることを特徴とする請求項 11 に記載の車両セキュリティ装置。

【請求項 20】 前記車両コントロール装置内の送信手段と協動するように前記キーシリンダに配設された発光素子を備え、前記車両用リモコン装置内の受信回路は、受光素子を含み、前記暗号元コードは、光信号からなり、前記受光素子を介して前記受信回路に送信されることを特徴とする請求項 11 に記載の車両セキュリティ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、メカニカルキー（以下、単に「キー」という）に内蔵された車両用リモコン装置を用いて専用の暗号化コードおよび ID コードを送信し、車両に搭載された車両コントロール装置と協動して、遠隔操作によるドアロック制御を行うとともにエンジン始動許可を行うための車両用リモコン装置および車両セキュリティ装置に関するものである。

【0002】

【従来の技術】 近年、自動車の盗難事件は著しく増加する傾向にあり、セキュリティ度の高い盗難防止装置の実現が要求されている。そこで、従来より、車両のドアロックをリモコン制御で解除する車両用リモコン装置や、車両の盗難防止のために、車両との間で暗号化コードを介して通信を行う車両用リモコン装置、およびこれを用いた車両セキュリティ装置などが種々提案されている。

【0003】 たとえば、盗難防止を目的とした周知のイモビライザ（エンジン不正始動防止）装置においては、エンジン始動用のキーシリンダ内にキーを挿入するのみではエンジンが始動されず、キー内の回路から送信される ID コードが車両内のコントロール装置に格納された ID コードと一致したときのみエンジン始動され、両者が異なる場合にはエンジン始動を禁止するようになっている。

【0004】 また、リモコン操作でドアロックの施錠および解除などを行う周知のキーレスエントリ装置においては、リモコン装置を内蔵したキーから所定の暗号化コードが車両コントロール装置に送信されない限り、たとえばドアロックが解除されないようになっている。

【0005】 図 12 はたとえば特開平 8-86130 号公報に記載された従来の車両セキュリティ装置を概略的に示すブロック構成図であり、キー側と車両側との間の送受信情報に基づいてエンジンの始動を許可してよい可否かを判断するイモビライザ機能を具備した場合を示している。

【0006】 図 12 において、イモビライザ装置として機能する車両セキュリティ装置は、エンジン不正始動防止用の ID コードなどが書き込まれたトランスポンダ 11A と、トランスポンダ 11A が内蔵されたキー 10 と、車両（図示せず）側に設けられてコイルアンテナ 20 と、コイルアンテナ 20 を有するキーシリンダ 21 と、車両に搭載されたマイクロコンピュータからなる車両コントロール装置 30A と、車両コントロール装置 30A により制御されるエンジン制御装置 29 とを備えている。

【0007】 車両コントロール装置 30A は、キーシリンダ 21 内でのキー 10 の操作に応答するとともに送受信データの処理を行う CPU からなる制御回路 25 と、制御回路 25 の記憶手段となる EEPROM（電氣的に消去可能な PROM）26 と、制御回路 25 とエンジン制御装置 29 との間に挿入されたエンジン通信補助回路 28 と、制御回路 25 とコイルアンテナ 20 との間に挿入された RF 送受信回路 23A とを含んでいる。車両コントロール装置 30A は、車両バッテリー 34 から供給された電力により動作する。

【0008】 通常、キー 10 をキーシリンダ 21 に挿入すると、メカニカルスイッチによりキーシリンダ 21 からキー検出信号 K が生成されて制御回路 25 に入力され

る。これにより、制御回路25は、キー10の挿入操作を認識して、RF送受信回路23Aからトランスポンダ11Aに向けて特定のIDコードを送信する。これに回答して、トランスポンダ11Aは、コイルアンテナ20に向けて特定のIDコードを送信する。

【0009】車両コントロール装置30A内のRF送受信回路23Aは、キー10内のトランスポンダ11Aからコイルアンテナ20を介して受信されたIDコードを制御回路25に入力する。

【0010】制御回路25は、EEPROM26内にあらかじめ格納されたIDコードと、受信されたIDコードとを比較し、エンジンの始動を許可してよいかの判定を行う。これにより、他人のキーでエンジンが始動されることが防止され、盗難を防止することができる。

【0011】図12のように、トランスポンダ11Aを内蔵したキー10と、コイルアンテナ20を介してキー10と通信を行う車両コントロール装置30Aとを備えたイモビライザ装置は、ドアロックをトランスポンダ11Aでリモコン解除するキーレスエントリ装置と、盗難防止用のイモビライザと、盗難防止アラーム装置とを

一体化することにより、コストパフォーマンスを向上させている。

【0012】また、図13はたとえば特開平8-149127号公報に記載された従来の車両セキュリティ装置を概略的に示すブロック構成図であり、ドアロックの開錠および施錠やトランクの解錠を通信するキーレスエントリ機能を具備した場合を示している。図13において、図12内と同様の構成には同一符号を付してその説明を省略する。

【0013】この場合、キーレスエントリ装置からなる車両セキュリティ装置は、キー10に内蔵されたCPUからなる車両用リモコン装置11Bと、受信用のアンテナ22を有する車両コントロール装置30Bと、車両コントロール装置30Bにより制御されるドアロック制御装置31とを備えている。

【0014】キー10内の車両用リモコン装置11Bは、キーレスエントリでドアロックの開錠などを行うためにユーザにより操作される手動スイッチ12と、車両用リモコン装置11BのCPU電源となる小形の電池13と、電池13から給電されるCPUすなわち制御回路14と、制御回路14の制御下でアンテナ22に向けて種々の暗号化コードCSを電波信号で送信する送信回路15と、制御回路14の記憶手段となるEEPROM17とを含んでいる。

【0015】車両用リモコン装置11B内のEEPROM17には、個々のキー10に対応して異なるIDコードおよび各通信動作毎に異なる暗号化コードCSが記憶されており、これらの暗号化コードCSのデータは、送信毎に制御回路14により呼び出されるようになっている。

【0016】また、車両コントロール装置30Bは、車両用リモコン装置11Bから送信されたIDコードおよび暗号化コードCSを受信する受信回路23と、受信データに回答してドアロック制御装置31を制御する制御回路25と、制御回路25に属するEEPROM26と、制御回路25と車載機器との間に挿入された入出力インターフェース27とを含んでいる。

【0017】入出力インターフェース27は、車両のルーム内のランプ32および車両のドア35に接続されており、制御回路25の制御下で、ドア35の開閉スイッチのオンオフ状態に応じて、ドア35の開放を示す場合にランプ32を点灯駆動するようになっている。

【0018】図13に示した車両セキュリティ装置は、電波信号（または、赤外線）からなる暗号化コードCSのデータを、車両用リモコン装置11B側の送信回路15から車両側の受信回路23に送信し、ドアロック制御装置31に対してドアロックの開錠および施錠や、トランクの解錠を通信する。また、この場合、暗号化コードCSのコード番号を変更して解読を困難にし、盗難防止機能をさらに確実にしている。

【0019】しかしながら、上記の各車両セキュリティ装置は、イモビライザ装置（図12参照）とキーレスエントリ装置（図13参照）とが独立して構成されており、相互に連絡を持つことがないので、イモビライザ機能およびキーレスエントリ機能の両方を達成するためには、各装置を個別に装着する必要がある。

【0020】このため、自動車メーカーでは、車載装置としての取り付け場所を確保する必要があるうえ接続配線が増加することから、各装置の取り付けコストが増加し、メンテナンスにおいても個別に労力を費やすことが余儀なくされている。

【0021】また、キーレスエントリ装置における電波信号の単方向通信を用いて、イモビライザ機能に兼用することも考えられるが、エンジン始動を許可（エンジン始動禁止を解除）するためには、ユーザによるキーレスエントリ操作が必須となるうえ、もし決められた時間内にエンジンを始動させないと、再びキーレスエントリ操作が必要になってしまうので実用的ではない。

【0022】また、キーレスエントリ装置の単方向通信において、送信データ（暗号化コードCS）を毎回固定させる方法では、盗聴解読を確実に防止することはできない。また、送信データの数値に対して簡単な増減を付加するのみでは、やはり送信データの盗聴解読や送信データのコピーなどを確実に防止することはできず、不正にエンジン始動されて車両盗難等の被害を受ける可能性もある。

【0023】さらに、上記特開平8-86130号公報（図12参照）に記載されたイモビライザ装置の簡易的な送受信装置（トランスポンダ11A）と、キーレスエントリ装置の送信回路15（図13参照）との両方を合

わせ持つ回路をキー10内に構成したとしても、図12および図13に個々に示したキー10を単に組み合わせたものと同等のコストがかかるので、コスト的にメリットが発生する見込みはほとんどない。

#### 【0024】

【発明が解決しようとする課題】従来の車両用リモコン装置および車両セキュリティ装置は以上のように、イモビライザ機能およびキーレスエントリ機能が個々の装置として独立しており、各機能が相互に連絡を持つことがないので、単に両機能を組み合わせたとしても、たとえばエンジンを始動する場合に必ずキーレスエントリ操作を実行しなければならず、セキュリティ度、操作性およびコストパフォーマンスを十分に向上させることができないという問題点があった。

【0025】この発明は上記のような問題点を解決するためになされたものであり、イモビライザ機能およびキーレスエントリ機能を統合してキー内に一体化することにより、材料コストの低減、組み付けコストの低減およびメンテナンス労力の低減を実現した車両用リモコン装置を得ることを目的とする。

【0026】また、この発明は、上記車両用リモコン装置と協働して、同様にイモビライザ機能およびキーレスエントリ機能を統合して一体化した車両コントロール装置を用いることにより、材料コストの低減、組み付けコストの低減およびメンテナンス労力の低減を実現した車両セキュリティ装置を得ることを目的とする。

【0027】また、この発明は、車両用リモコン装置に受信回路を設けてイモビライザ用の双方向通信機能を確保するとともに、他のキーに対して解読困難な毎回異なる暗号元コードおよび暗号化コードの送受信することにより、送信データの盗聴解読コピーによる不正なエンジン始動および車両盗難などの被害を確実に防止し、セキュリティ度をさらに向上させた車両用リモコン装置および車両セキュリティ装置を得ることを目的とする。

【0028】さらに、この発明は、キーレスエントリ装置および送信回路を共用して部品点数を削減することにより、十分な低コスト化を実現するとともに、暗号化コードの利用におけるセキュリティ度の向上を実現した車両用リモコン装置および車両セキュリティ装置を得ることを目的とする。

#### 【0029】

【課題を解決するための手段】この発明に係る車両用リモコン装置は、車両のエンジン始動用のキーシリンダに挿入されるキーに内蔵され、且つ車両との間で相互に通信を行う車両用リモコン装置であって、キーシリンダへのキーの挿入時に車両側から送信される暗号元コードを受信する受信回路と、暗号元コードを記憶する記憶回路と、ユーザにより操作される手動スイッチと、暗号元コードの受信にตอบสนองして第1の暗号化コードを生成するとともに、手動スイッチの操作にตอบสนองして第2の暗号化コ

ードを生成する制御回路と、第1および第2の暗号化コードを電波信号により車両側に送信する送信回路とを備え、第1の暗号化コードは、車両のエンジン始動を許可するための指令を含み、第2の暗号化コードは、記憶回路内の暗号元コードに基づいて生成され、車両のドアロックの施錠または開錠するための指令を含むものである。

【0030】また、この発明に係る車両用リモコン装置は、暗号元コードは、車両を特定するために設定されたトリガ信号を含み、制御回路は、トリガ信号に基づいて暗号元コードの正規を判定するとともに、トリガ信号にตอบสนองして第1の暗号化コードを生成し、記憶回路は、正規と判定された暗号元コードのみを記憶するものである。

【0031】また、この発明に係る車両用リモコン装置は、制御回路は、記憶回路に記憶された暗号元コードに基づいて、通信毎に異なる第2の暗号化コードを生成するものである。

【0032】また、この発明に係る車両用リモコン装置は、第1および第2の暗号化コードは、互いに異なるものである。

【0033】また、この発明に係る車両用リモコン装置は、第1の暗号化コードの電波出力は、第2の暗号化コードの電波出力よりも小さく設定されたものである。

【0034】また、この発明に係る車両用リモコン装置は、暗号元コードは、電波信号からなり、受信回路は、インダクタンスを有するコイルとキャパシタンスを有するコンデンサとからなる共振回路を含み、共振回路を介した電磁結合により暗号元コードを受信するものである。

【0035】また、この発明に係る車両用リモコン装置は、暗号元コードは、磁気信号からなり、受信回路は、磁気抵抗素子を含み、磁気抵抗素子を介して暗号元コードを受信するものである。

【0036】また、この発明に係る車両用リモコン装置は、暗号元コードは、磁気信号からなり、受信回路は、ホールセンサを含み、ホールセンサを介して暗号元コードを受信するものである。

【0037】また、この発明に係る車両用リモコン装置は、暗号元コードは、光信号からなり、受信回路は、受光素子を含み、受光素子を介して暗号元コードを受信するものである。

【0038】また、この発明に係る車両用リモコン装置は、暗号元コードは、電波信号からなり、受信回路は、高周波受信回路からなるものである。

【0039】また、この発明に係る車両用リモコン装置を用いた車両セキュリティ装置は、車両用リモコン装置が内蔵されたキーと、車両に設けられて、キーの挿入時にキー検出信号を生成するキーシリンダと、車両に搭載されて、車両用リモコン装置との間で相互に通信を行う

車両コントロール装置とを備え、車両コントロール装置は、車両用リモコン装置から送信される第1および第2の暗号化コードを受信する受信手段と、キー検出信号に応答して暗号元コードを生成するとともに、第1および第2の暗号化コードの受信に応答して車両のエンジンおよびドアを制御する制御手段と、暗号元コードを車両用リモコン装置に送信するための送信手段とを含み、制御手段は、第1の暗号化コードに応答して車両のエンジン始動を許可するとともに、第2の暗号化コードに応答して車両のドアロックを制御するものである。

【0040】また、この発明に係る車両セキュリティ装置は、制御手段は、通信毎に異なる暗号元コードを生成するものである。

【0041】また、この発明に係る車両セキュリティ装置は、制御手段は、通信毎ランダムカウンタ値を用いて暗号元コードを生成するものである。

【0042】また、この発明に係る車両セキュリティ装置は、暗号元コードは、第1の暗号化コードの送信要求を車両用リモコン装置に指令するためのトリガ信号を含むものである。

【0043】また、この発明に係る車両セキュリティ装置は、トリガ信号は、車両を特定するために設定された複数のデータの組み合わせからなるものである。

【0044】また、この発明に係る車両セキュリティ装置は、車両コントロール装置内の制御手段は、第2の暗号化コードに応答して、車両のドアロックを制御するとともに、車両のエンジン始動を許可するものである。

【0045】また、この発明に係る車両セキュリティ装置は、車両用リモコン装置内の制御回路は、第2の暗号化コードを送信毎に変更し、車両コントロール装置内の制御手段は、第2の暗号化コードを受信毎に変更し、車両コントロール装置は、受信毎に変更される第2の暗号化コードを記憶する記憶手段を含み、制御手段は、受信された第2の暗号化コードと、記憶手段に記憶された第2の暗号化コードとの差が一定範囲以内のときに、受信された第2の暗号化コードを正規と判定し、正規と判定された第2の暗号化コードのみに応答して、車両のドアロックを制御するものである。

【0046】また、この発明に係る車両セキュリティ装置は、車両コントロール装置内の送信手段と協動するようにキーシリンダに配設されたリング状のコイルアンテナを備え、車両用リモコン装置内の受信回路は、インダクタンスを有するコイルとキャパシタンスを有するコンデンサとからなる共振回路を含み、暗号元コードは、電波信号からなり、共振回路を介した電磁結合により、コイルアンテナから受信回路に送信されるものである。

【0047】また、この発明に係る車両セキュリティ装置は、車両コントロール装置内の送信手段と協動するようにキーシリンダに配設された磁石手段を備え、暗号元コードは、磁気信号からなり、磁気応答作用により磁石

手段を介して車両用リモコン装置内の受信回路に送信されるものである。

【0048】また、この発明に係る車両セキュリティ装置は、車両コントロール装置内の送信手段と協動するようにキーシリンダに配設された発光素子を備え、車両用リモコン装置内の受信回路は、受光素子を含み、暗号元コードは、光信号からなり、受光素子を介して受信回路に送信されるものである。

【0049】

#### 10 【発明の実施の形態】

実施の形態1. 以下、この発明の実施の形態1を図について説明する。図1はこの発明の実施の形態1による車両セキュリティ装置を示すブロック構成図であり、車両用リモコン装置およびこの相手側となる車両コントロール装置を概略的に示している。

【0050】図1において、図12および図13内に示したものと同様の構成には同一符号を付してその説明を省略する。この発明の実施の形態1による車両セキュリティ装置は、キー10に一体構成された車両用リモコン装置11と、車両に搭載された車両コントロール装置30とから構成されている。

【0051】車両コントロール装置30の入力側には、前述(図12参照)と同様に、キーシリンダ21が接続されており、キーシリンダ21の挿入口には、車両用リモコン装置11を内蔵したキー10が挿入されるようになっている。

【0052】この場合、車両コントロール装置30内の制御回路25は、キー検出信号Kに応答してイモビライザ用の暗号元コードCRを生成するとともに、暗号元コードCRを車両用リモコン装置11に送信する毎に、セキュリティ度の高いランダムカウンタ値を用いて暗号元コードCRを変更する。

【0053】また、車両用リモコン装置11内の制御回路14は、暗号元コードCRに応答してイモビライザ用の第1の暗号化コードCS1を生成するとともに、手動スイッチ12の操作に応答して、暗号元コードCRに基づくキーレスエントリ用の第2の暗号化コードCS2を生成し、暗号化コードCS2を車両コントロール装置30に送信する毎に、簡単な演算(データ数値のインクリメント)により暗号化コードCS2を変更する。

【0054】第1および第2の暗号化コードCS1およびCS2は、互いに異なるランダムコードを含んでいるが、キーレスエントリ時に車両から離れて送信される第2の暗号化コードCS2は、イモビライザ時にキーシリンダ21内で送信される第1の暗号化コードCS1よりも、必要最小限の範囲内で送信電波出力が大きくなるように設定されている。

【0055】また、各制御回路内のEEPROM17および26には、最新のイモビライザ動作時に設定された暗号元コードCRが記憶されるとともに、必要に応じて



暗号元コードCRに対応した第1および第2の暗号化コードも記憶される。

【0056】車両コントロール装置30は、制御回路25を中心として、イモビライザ用の第1の暗号化コードCS1およびキーレスエントリ用の第2の暗号化コードCS2（ここでは、総称して、暗号化コードCSと記す）を電波信号で受信する受信回路23と、イモビライザ用の暗号元コードCRを送信するための送信回路24と、現在の暗号元コードCRおよびこの暗号元コードCRに基づく暗号化コードCSを記憶するEEPROM26とを有する。

【0057】また、車両コントロール装置30は、制御回路25とエンジン制御装置29との間でイモビライザ用の双方向通信を行うエンジン通信補助回路28と、制御回路25からドアロック制御装置31に対してキーレスエントリ用のドアロック制御信号DLを出力する入出力インターフェース27とを有する。

【0058】EEPROM26内の暗号元コードCRは、イモビライザ動作毎に呼び出されて車両用リモコン装置11に送信されるとともに、後述するように、送信後に演算更新されて再記憶される。暗号元コードCRおよび暗号化コードCSは、後述するトリガ信号およびキー操作毎のIDコードなどを含む。

【0059】入出力インターフェース27は、ドアロック制御装置31からの操作確認用の応答信号（図示せず）を取り込むとともに、同様に、車両ルーム照明用のランプ32およびクラクション用のホーン33に駆動制御信号を出力して、ランプ32およびホーン33からの応答信号を取り込む。

【0060】また、エンジン通信補助回路28は、制御回路25からの始動許可信号STをエンジン制御装置29に送信するとともに、エンジン制御装置29からの操作確認用の応答信号REを受信して制御回路25に入力する。

【0061】キーシリンダ21の挿入口に設けられたコイルアンテナ20は、車両用リモコン装置11に向けてイモビライザ用の暗号元コードCRを送信するとともに、車両用リモコン装置11から送信された暗号化コードCSを受信する。また、キーシリンダ21は、キーシリンダ21に挿入されたキー10が所定の動作位置にあることをメカニカルに検出し、キー検出信号Kを制御回路25に入力する。

【0062】一方、キー10内の車両用リモコン装置11は、前述の手動スイッチ12、電池13、制御回路14、送信回路15およびEEPROM17とともに、コイルアンテナ20から送信されてくるイモビライザ用の暗号元コードCRを受信するための受信回路16を有する。

【0063】前述（図13参照）と同様に、手動スイッチ12は、キーレスエントリ時において、ドアロックの

開錠または施錠を行うために外部から操作される。また、車両用リモコン装置11内には、キーレスエントリ時の暗号化コードの送信動作などを行う制御回路14の電源として、電池13が設けられている。

【0064】この場合、送信回路15は、制御回路14の制御下で、EEPROM17に記憶された暗号元コードCRに基づく暗号化コードCSを電波信号により送信し、コイルアンテナ20を介して車両コントロール装置30内の受信回路23に送信する。

【0065】また、受信回路16は、イモビライザ動作時に車両コントロール装置30内の送信回路24からコイルアンテナ20を介して送信される暗号元コードCRを電波信号により受信する。

【0066】車両用リモコン装置11内の制御回路14は、車両コントロール装置30から暗号元コードCR（トリガ信号および暗号データを含む）が受信されたときに、トリガ信号から暗号元コードCRの正規を判定し、正規判定された暗号元コードCRのみをEEPROM17に更新記憶させる。

【0067】したがって、EEPROM17には、前回のイモビライザ動作時に車両コントロール装置30から送信された最新の暗号元コードCRが常に記憶されており、現在の暗号元コードCRに応じた暗号化コードCS（IDコードなどを含む）も更新記憶され得る。

【0068】EEPROM17に記憶された暗号化コードCSは、イモビライザ動作時の暗号元コードCRに応じた送信タイミング、およびキーレスエントリ動作時の送信タイミング毎に制御回路14から呼び出される。

【0069】図2は図1内の受信回路16を具体的に示すブロック図であり、ここでは、受信回路16が電磁結合作用を用いた回路により構成された場合を示している。図2において、受信回路16は、インダクタンスを有するコイル16aと、キャパシタンスを有するコンデンサ16bと、整流部16cとを備えている。

【0070】コイル16aおよびコンデンサ16bは、互いに並列接続されて共振回路を構成しており、電磁結合を介して暗号元コードCRを受信する。整流部16cは、共振回路と制御回路14との間に挿入されており、共振回路16aおよび16bで受信された暗号元コードCR（交流信号）を整流して制御回路14に入力する。

【0071】図3は車両コントロール装置30から送信されるイモビライザ用の暗号元コードCRに含まれるトリガ信号の波形パターン例を示す説明図である。トリガ信号は個々の車両に応じて異なり、たとえば図3において、トリガ信号Taは単純な矩形波からなる場合、トリガ信号Tbは複数のパルス列からなる場合をそれぞれ示している。

【0072】各車両を個別に特定するためのトリガ信号は、図3の波形例（Ta、Tb）に限らず、暗号元コードCR内の最初の数ビット（図3の例では、9ビット）



からなる任意の組み合わせデータにより構成されている。

【0073】トリガ信号は、車両コントロール装置30内のEEPROM26内にあらかじめ設定されており、最初のイモビライザ用の送信時に車両用リモコン装置11内のEEPROM17に記憶される。また、暗号元コードCR内のトリガ信号は、車両用リモコン装置11に対して、第1の暗号化コードCS1の送信を要求する指令信号としても機能する。

【0074】なお、暗号元コードCRのランダムデータ（図示せず）は、トリガ信号Ta、Tbに続く複数ビット（たとえば、20ビット程度）からなり、種々の制御指令内容やIDコードなどを含んでいる。

【0075】車両用リモコン装置11内の制御回路14は、電池13を電源として動作し、手動スイッチ12の接点信号に応答してEEPROM17内の暗号元コードCRから第2の暗号化コードCS2を作成し、これを送信回路15から電波信号として送信するキーレスエントリ機能と、車両コントロール装置30からの暗号元コードCRを受信回路16で受信し、第1の暗号化コードCS1を車両コントロール装置30に自動的に送信するイモビライザ機能とを有する。

【0076】車両コントロール装置30内の制御回路25は、車両バッテリー34を電源として動作し、キーシリンダ21へのキー挿入によるキー検出信号Kに응答して暗号元コードCRを送信回路24からコイルアンテナ20を介して送信し、車両用リモコン装置11からの応答信号（第1の暗号化コードCS1）を受信回路23で受信する。

【0077】これにより、制御回路25は、受信された第1の暗号化コードCS1をEEPROM26内のデータと比較し、第1の暗号化コードCS1が正規と判定されたときにエンジン制御装置29に始動許可信号STを通信するイモビライザ機能を有する。

【0078】また、制御回路25は、第2の暗号化コードCS2が受信されたときに、入出力インターフェース27を介して、ドアロック制御装置31にドアロック制御信号DLを出力するキーレスエントリ機能を有する。さらに、制御回路25は、ドアロック動作状態をユーザに知らせるために、車両ルーム内のランプ32またはクラクション用のホーン33を駆動する機能を有する。

【0079】次に、図4および図5のフローチャートを参照しながら、図1～図3に示したこの発明の実施の形態1による車両セキュリティ装置の処理動作について説明する。

【0080】図4はキー10に内蔵された車両用リモコン装置11における動作を示し、図4において、S41～S48はイモビライザ装置として機能する場合の処理ステップであり、S40、S49およびS50は、キーレスエントリ装置として機能する場合の処理ステップで

ある。

【0081】同様に、図5は車両コントロール装置30における動作を示し、図5において、S61～S68はイモビライザ装置として機能する場合の処理ステップであり、S60およびS69～S71は、キーレスエントリ装置として機能する場合の処理ステップである。

【0082】最初に、図4内のステップS41～S48にしたがって、車両用リモコン装置11によるイモビライザ装置としての動作について説明する。なお、車両用リモコン装置11内のEEPROM17には、車両コントロール装置30内のEEPROM26と同一の暗号元コードCRがあらかじめ記憶されているものとする。

【0083】まず、車両用リモコン装置11内の制御回路14は、手動スイッチ12がオン操作されているか否かを判定し（ステップS40）、もし、オン操作されていない（すなわち、NO）と判定されれば、続いて、キー10が車両のキーシリンダ21に挿入されたか否かを判定する（ステップS41）。

【0084】もし、キー10がキーシリンダ21に挿入されていない（すなわち、NO）と判定されれば、ステップS40に戻り、キー10の挿入待機状態となる。一方、エンジン始動時において、ユーザが、手動スイッチ12を操作することなく、キー10をキーシリンダ21に挿入して回転操作すると、ステップS41において、キー10がキーシリンダ21に挿入された（すなわち、YES）と判定される。

【0085】キー10の挿入により、キーシリンダ21からは、キー検出信号Kが生成されて車両コントロール装置30に入力される。これにより、車両コントロール装置30内の制御回路25は、イモビライザ動作毎に変更されたランダムデータを含む暗号元コードCR（後述する）を生成する。このとき、トリガ信号は変更されない。

【0086】続いて、車両用リモコン装置11内の制御回路14は、キーシリンダ21に設けられたコイルアンテナ20から暗号元コードCRが受信されたか否かを判定し（ステップS42）、もし、暗号元コードCRが受信された（すなわち、YES）と判定されれば、受信された暗号元コードCRとEEPROM17に記憶された暗号元コードとを比較し、双方のトリガ信号が一致するか否かにより、暗号元コードCRが正規か否かを判定する（ステップS43）。

【0087】もし、暗号元コードCRが正規でない（すなわち、NO）と判定されればステップS40に戻り、また、暗号元コードCRが正規である（すなわち、YES）と判定されれば、今回受信された暗号元コードCRをEEPROM17に更新記憶させる（ステップS44）。

【0088】このとき、暗号元コードCRには、前述のように車両毎に異なるトリガ信号が含まれており、たと

例えば自車両のトリガ信号がパルス状のトリガ信号Tb  
(図3参照)であれば、単純な矩形波からなるトリガ信号Taが受信されても不一致と判定される。

【0089】したがって、不一致の場合には、車両のエンジン始動禁止状態(後述する)が解除されず、盗難を防止することができる。また、自車両の同様の車両セキュリティ装置を用いた他車両が近傍に存在しても、相互の使用コードを区別可能なので、自車両を確実に特定して誤動作を防止することができる。

【0090】続いて、暗号元コードCR内のトリガ信号により、暗号元コードCRが第1の暗号化コードCS1の送信を要求しているか否かを判定し(ステップS45)、もし、暗号元コードCRが暗号化コードCS1の送信要求を示す(すなわち、YES)と判定されれば、EEPROM17に既に記憶された暗号元コードCRに基づいて第1の暗号化コードCS1を作成する(ステップS46)。

【0091】このように、あらかじめ共通データとして車両用リモコン装置11および車両コントロール装置30に記憶されたトリガ信号を照合し(ステップS43)、正規信号と判定されたときに、EEPROM17に新たに記憶された暗号元コードCRを用いて、イモビライザ応答コードとして第1の暗号化コードCS1を作成する(ステップS46)。

【0092】こうして生成された暗号化コードCS1は、送信回路15から送信され、キーシリンダ21側のコイルアンテナ20を介して車両コントロール装置30に入力される(ステップS47)。

【0093】最後に、制御回路14に印加される電池13の電圧(CPU入力電圧)が規定電圧以上か否かを判定し(ステップS48)、もし、電池13の電圧が正常(すなわち、YES)と判定されれば、最初の手動スイッチ12の操作確認ステップS40に戻る。

【0094】また、電池13が消耗して電池電圧が規定電圧未満に低下した(すなわち、NO)と判定されれば、図4内のイモビライザ処理ルーチンを終了する。この場合、車両用リモコン装置11の動作不良やデータ異常などが発生するので、これを未然に防止するために電池13の交換が行われる。

【0095】一方、ステップS42において、車両コントロール装置30から暗号元コードCRが受信されない(すなわち、NO)と判定された場合は、以下のステップS43～S47をスキップして、暗号化コードCS1を送信せずにステップS48に進む。

【0096】また、ステップS45において、暗号元コードCRが送信要求を示していない(すなわち、NO)と判定された場合は、以下のステップS46およびS47をスキップして、暗号化コードCS1を送信せずにステップS48に進む。

【0097】以上のイモビライザ機能の処理動作は、エ

ンジン始動時にユーザがキー10をキーシリンダ21に挿入して回転操作し、エンジンを始動させるまでの数100m秒の間に自動的に実行される。また、イモビライザ機能は、後述するキーレスエントリ機能とは独立しているので、ユーザによる特別な操作は何ら必要としない。

【0098】なお、ここでは図示しないが、車両用リモコン装置11における暗号元コードCRの受信時間および暗号化コードCS1の演算時間などを考慮して、車両コントロール装置30側から、次のエンジン始動時の暗号化コードCS1の演算用の暗号元コードCRが送信されてもよい。

【0099】この場合、制御回路14は、受信回路16から受信された暗号元コードCRが次の暗号化コードの演算要求を示していれば、これに応答して、あらかじめ次の暗号化コードCS1の演算を行い、これをEEPROM17に記憶しておくことになる。これにより、イモビライザ機能での通信時間とデータ照合時間を短縮することができる。

【0100】次に、図5内のステップS61～S68にしたがって、車両に搭載された車両コントロール装置30によるイモビライザ用の処理動作について説明する。なお、車両のエンジンは、始動前において始動禁止状態に設定制御されているものとする。

【0101】まず、車両コントロール装置30内の制御回路25は、車両用リモコン装置11側から暗号化コードCS(第1または第2の暗号化コード)が受信されたか否かを判定し(ステップS60)、もし、暗号化コードCSが全く受信されていない(すなわち、NO)と判定されれば、キーシリンダ21からのキー検出信号Kが入力されたか否かを判定する(ステップS61)。

【0102】もし、キー検出信号Kが入力されていない(すなわち、NO)と判定されればステップS60に戻り、暗号化コードCSの受信待機状態およびキー10の挿入待機状態となる。一方、キー検出信号Kが入力された(すなわち、YES)と判定されれば、第1の暗号化コードCS1の送信要求を示す暗号元コードCRを、送信回路23およびコイルアンテナ20を介して車両用リモコン装置11に送信する(ステップS62)。

【0103】すなわち、エンジン始動時にキー10がキーシリンダ21内に挿入されて回転操作されると、制御回路25は、キー検出信号Kによりキー10が挿入されたことを認識し、あらかじめEEPROM26内に記憶されている暗号元コードCRを電波信号に変換して送信する。

【0104】続いて、ステップS62の実行後から、セキュリティ用の一定時間が経過(タイムオーバー)したか否かを判定し(ステップS63)、もし、タイムオーバーしていない(すなわち、NO)と判定されれば、この一定時間以内に車両用リモコン装置11からの応答に

より第1の暗号化コードCS1が受信されたか否かを判定する(ステップS64)。

【0105】もし、ステップS63においてタイムオーバー(すなわち、YES)と判定されるか、またはステップS64において暗号化コードCS1が受信されない(すなわち、NO)と判定されれば、一定時間以内に暗号化コードCS1が受信されない状態と見なし、そのまま図5内のイモビライザ処理ルーチンから抜け出る。したがって、この場合、エンジンの始動禁止状態は維持される。

【0106】一方、ステップS64において、第1の暗号化コードCS1が受信された(すなわち、YES)と判定されれば、受信された暗号化コードCS1と、あらかじめ演算されてEEPROM26内に記憶された暗号化コードとを比較し、両者が一致するか否かにより暗号化コードCS1が正規か否かを判定する(ステップS65)。

【0107】もし、両者が一致しており、暗号化コードCS1が正規である(すなわち、YES)と判定されれば、制御回路25は、エンジン通信補助回路28を介して、エンジン制御装置29に対して始動許可信号STを出力し、エンジンの始動許可(始動禁止解除)を示す指令コードを通信する(ステップS66)。

【0108】これにより、通常のエンジン始動が可能な状態となり、以下、キー10のキーシリンダ21内での回転操作により、実際にエンジンが始動される。最後に、セキュリティ度を向上させるために、毎回ランダムに発生する数値を次回の暗号元コードCRとしてEEPROM26に記憶させ(ステップS67)、図5の処理ルーチンを抜け出てイモビライザ動作を終了する。

【0109】一方、ステップS65において、受信された暗号化コードCS1がEEPROM26内の暗号化コードと一致せず、暗号元コードCRが正規でない(すなわち、NO)と判定されれば、ユーザへの警告としてルーム内のランプ32を点滅させ(ステップS68)、図5の処理ルーチンを抜け出てイモビライザ動作を中止させる。

【0110】図5においては、次回の暗号元コードCRを演算記憶するステップS67が実行された時点でイモビライザ処理を完了しているが、ステップS67に続いて、次回の暗号元コードCRを車両用リモコン装置11側に送信してもよい。

【0111】この場合、前述のように、車両用リモコン装置11側において、データ送受信および暗号化演算などを前もって実行することができるので、次回のイモビライザ動作時において、車両用リモコン装置11へのデータ送信時間や車両用リモコン装置11および車両コントロール装置30内での演算時間を短縮することができる。

【0112】なお、暗号元コードCRに応じた暗号化コ

ードCS1は、車両用リモコン装置11および車両コントロール装置30において同一の暗号化手順により作成される。具体的な暗号化手順としては、たとえば「現代暗号化理論」(電子情報通信学会編纂)の第3章に記載されている「データ暗号化規格(通称:DES(Data Encryption Standard))」などに準拠することができる。

【0113】上記文献によれば、一般に、暗号化手順が未知の場合には、暗号化コードを復元することは不可能に近いとされているので、たとえば暗証番号や個別IDなどのデータセキュリティが非常に優れていることが分かる。

【0114】次に、図4内のステップS40、S49およびS50にしたがって、車両用リモコン装置11によるキーレスエントリ用の処理動作について説明する。まず、ドアロック解除などのキーレスエントリ操作時において、ユーザは、キー10をキーシリンダ21に挿入することなく、車両から離れた位置でキー10を所持して手動スイッチ12をオン操作する。

【0115】このとき、車両用リモコン装置11内の制御回路14は、ステップS40において、手動スイッチ12がオン操作された(すなわち、YES)と判定し、キーレスエントリ用の第2の暗号化コードCS2をEEPROM17から読み出して送信回路15から送信する(ステップS49)。

【0116】第2の暗号化コードCS2は、EEPROM17に記憶された現在の暗号元コードCRに基づいて、イモビライザ用の第1の暗号化コードCS1とは異なる演算により生成される。車両用リモコン装置11から送信された第2の暗号化コードCS2は、コイルアンテナ20から受信回路23を介して受信され、車両コントロール装置30内の制御回路25に入力される。

【0117】続いて、制御回路14は、第2の暗号化コードCS2の送信(ステップS49)を完了した後、EEPROM17に記憶された暗号元コードCRを用いて、次回のキーレスエントリ用の暗号化コードCS2を求めてEEPROM17に記憶させる(ステップS50)。

【0118】このとき、次回の第2の暗号化コードCS2は、簡単な演算、たとえば現在の暗号化コードCS2のデータ数値を+1(インクリメント)することにより求められ、キーレスエントリ動作を繰り返す毎に順次インクリメントされて、更新記憶される。一方、暗号元コードCRは、イモビライザ動作による更新が行われな限り変更されない。

【0119】したがって、キーレスエントリ用の暗号化コードCS2は、エンジン始動時のイモビライザ動作毎に車両コントロール装置30から送信されてくる暗号元コードCRを基準として簡単な演算で作成され、イモビライザ動作毎に大きく変更される。

【0120】このように、キーレスエントリ機能においても、データセキュリティ度を向上させ、暗号化コードCS2の盗聴者による車両トラブル（ドアロックの不法開閉など）を回避することができる。

【0121】なお、ドアロック開閉用のキーレスエントリ機能は、キー10側から車両側への単方向通信によるものであり、双方向通信を用いるイモビライザ機能と比べて重要度が低いので、今回の暗号化コードCR2のために複雑なランダム演算を用いる必要はない。今回のキーレスエントリ用の第2の暗号化コードCS2の記憶処理（ステップS50）が終了した後は、電源チェック用のステップS48に進む。

【0122】次に、図5内のステップS60、S69～S71にしたがって、車両コントロール装置30によるキーレスエントリ用の処理動作について説明する。まず、ユーザが手動スイッチ12をオン操作すると、車両用リモコン装置11側から第2の暗号化コードCS2が送信され、車両コントロール装置30内の制御回路25は、ステップS60において、ノイズ信号と区別可能な暗号化コードCSが受信された（すなわち、YES）と判定する。

【0123】続いて、制御回路25は、受信された暗号化コードCSと、EEPROM26に記憶された第2の暗号化コード（CS2）とを比較し、両者のトリガ信号の一致状態から暗号化コードCSの正規を判定するとともに、暗号化コードCS内のランダムデータから、受信された暗号化コードCSが、ドアロック関係の特定コードを示す（第2の暗号化コードCS2）か否かを判定する（ステップS69）。

【0124】もし、受信された暗号化コードCSが、正規でないと判定されるか、または、第2の暗号化コードCS2でない（すなわち、NO）と判定されれば、ステップS60に戻り、暗号化コードCSの受信待機状態となる。

【0125】一方、ステップS69において、受信された暗号化コードCS2が正規であって且つドアロック関係の特定コードを示す（すなわち、YES）と判定されれば、ドアロック制御装置31に対して、施錠（ドアロック）または開錠（ドアロック解除）を指令するためのドアロック制御信号DLを出力する（ステップS70）。

【0126】こうして、キーレスエントリ動作によるドアロック制御が行われた後、制御回路25は、前述の車両用リモコン装置11内の制御回路14と同様の演算方法、すなわち今回の暗号化コードCS2のデータ数値のインクリメント処理により、今回の暗号化コードCS2を計算してEEPROM26に記憶させ（ステップS71）、図5のキーレスエントリ処理ルーチンを抜ける。

【0127】図6はイモビライザ動作時の信号通信タイ

ミングを図式的に示す説明図であり、各装置11、29および30の間で時系列的な信号が双方向に送受信される状態を示している。

【0128】また、図7はキーレスエントリ動作時の信号通信タイミングを図式的に示す説明図であり、各装置11、30および31の間で時系列的な信号が単方向に送信される状態を示している。各図において、横軸は時間tである。

【0129】イモビライザ動作時において、図6に示すように、車両コントロール装置30から車両用リモコン装置11に暗号元コードCRが送信されると、これにตอบสนองして、車両用リモコン装置11から車両コントロール装置30に第1の暗号化コードCS1が送信される。

【0130】続いて、車両コントロール装置30からエンジン制御装置29に始動許可信号STが送信されると、エンジン制御装置29から車両コントロール装置30に応答信号REが送信されてエンジン始動が可能な状態になり、以下、キー10の操作によりエンジンが始動される。上記通信シーケンスは、イモビライザ動作毎に繰り返される。

【0131】一方、キーレスエントリ動作時において、図7のように、車両用リモコン装置11から車両コントロール装置30にドアロック操作要求を示す第2の暗号化コードCS2が送信されると、これにตอบสนองして、車両コントロール装置30からドアロック制御装置31にドアロック制御信号DLが出力される。

【0132】以下、ドアロック制御装置31により、ドアロックの施錠または開錠が行われる。図7から明らかなように、キーレスエントリ機能は、単方向通信により行われるので、応答性が速く、短時間の通信が可能になる。

【0133】このように、車両用リモコン装置11内に受信回路16を設けることにより、イモビライザ装置としての双方向通信が可能になり、キーレスエントリ装置の単方向通信と協働して、単一のキー10内において両装置を有効に一体化することができる。

【0134】また、イモビライザ装置およびキーレスエントリ装置の一体化により、集中管理が可能になることから、車両用リモコン装置11のメンテナンスが容易になるとともに、部品点数が削減されてコストダウンを実現することができる。

【0135】また、ユーザが2個の装置を個別に所持する必要がなくなるうえ、手動スイッチ12の操作は、キーレスエントリ時のみに行われて、イモビライザ時には不要となるので、操作性を簡潔化することができる。

【0136】また、イモビライザ時において、キーレスエントリ用の第2の暗号化コードCS2とは別の第1の暗号コードCS1を自動的に生成するので、イモビライザ装置として独立して機能することができ、エンジン始動時にキーレスエントリ操作を実行する必要はない。

【0137】また、車両コントロール装置30側もキーレスエントリ機能およびイモビライザ機能が一体化されているので、自動車メーカーにおける車両コントロール装置30の車両への取り付けスペースが軽減され、接続配線が減少してコストダウンが実現するうえ、取り付け後のメンテナンスにおいても、集中管理が可能となり労力が軽減される。

【0138】また、車両用リモコン装置11と車両コントロール装置30との間の通信データ（暗号元コードCRおよび暗号化コードCS）が暗号化されており、通信毎に異なるデータを送信することができるので、暗号化手法による解読や次回コードの予測が非常に困難になり、セキュリティ度が向上する。

【0139】特にイモビライザ時には、車両用リモコン装置11および車両コントロール装置30が双方向通信により暗号データを用いるので、毎回予測不可能なデータが送受信され、セキュリティ度がさらに向上する。

【0140】また、車両用リモコン装置11において、受信回路16内の共振回路16aおよび16bによる電磁結合を用いて暗号元コードCRを受信するので、受信回路16内は、電源を必要としないでデータ受信を行うことができる。

【0141】また、イモビライザ用の第1の暗号化コードCS1の電波出力を、キーレスエントリ用の第2の暗号化コードCS2の電波出力よりも小さく設定したので、電波信号の漏洩による暗号化コードCS1の盗聴を防止するとともに、電池13の消費電力を必要最小限に抑制することができる。

【0142】さらに、車両コントロール装置30から送信される暗号元コードCR内のトリガ信号を、トリガ信号TaまたはTb（図3参照）のように、複数のデータの組み合わせで設定することにより、自車両の特定を確実にすることができる。

【0143】実施の形態2. なお、上記実施の形態1では、制御回路25は、キーレスエントリ時の第2の暗号化コードCS2の正規判定ステップS69において、受信された暗号化コードCS2とEEPROM26内の暗号化コードCS2との一致を判定したが、両者の相違が一定範囲以内であれば一致と判定してもよい。

【0144】なぜなら、前述のように車両用リモコン装置11から送信される次の暗号化コードCS2は送信毎に異なるので、コイルアンテナ20との間の通信が不成立となる場合や、コイルアンテナ20との間の通信範囲外で手動スイッチ12を操作する場合には、キーレスエントリ対象が自車両であっても、車両用リモコン装置11から送信される暗号化コードCS2と、車両コントロール装置30内の暗号化コードCS2とが完全に一致せず、キーレスエントリ機能が達成できない状況が起こり得るからである。

【0145】したがって、この発明の実施の形態2にお

いては、車両用リモコン装置11から送信される暗号化コードCS2と、車両コントロール装置30内の暗号化コードCS2との各数値データとが完全に一致しない場合であっても、両者の違いが一定範囲以内であれば一致状態と判定する。これにより、通信状態が多少不完全な場合でも、キーレスエントリ機能が不実行となる可能性を低減させることができる。

【0146】実施の形態3. また、上記実施の形態1では、車両コントロール装置30から車両用リモコン装置11に暗号元コードCRを送信するために電波信号を用いたが、磁気信号を用いてもよい。以下、暗号元コードCRを磁気信号で送信するようにしたこの発明の実施の形態3を図について説明する。

【0147】図8はこの発明の実施の形態3による車両用リモコン装置11の構成を示すブロック図であり、図8において、受信回路16Aは、受信部となる磁気抵抗素子16dと、データ検出用の信号検出部16eとを備えている。

【0148】磁気抵抗素子16dは、コイルアンテナ20から磁気信号で送信される暗号元コードCRを受信して電気信号に変換する。続いて、信号検出部16eは、磁気抵抗素子16dから出力される電気信号から、特定データを検出して制御回路14に入力する。

【0149】図8のように、暗号元コードCRを磁気信号で送信した場合、コイルアンテナ20をそのまま電磁石として送信手段に用いることができる。また、コイルアンテナ20に代えて永久磁石（図示せず）を用いれば、車両コントロール装置30側の消費電力を節約することができる、コスト低減を実現することができる。

【0150】実施の形態4. また、上記実施の形態3では、磁気信号からなる暗号元コードCRを磁気抵抗素子16dを介して受信したが、ホール素子を介して受信してもよい。以下、車両用リモコン装置11内の受信回路にホールセンサを設けたこの発明の実施の形態4を図について説明する。

【0151】図9はこの発明の実施の形態4による車両用リモコン装置11の構成を示すブロック図であり、図9において、受信回路16Bは、受信部となるホールセンサ16fと、データ検出用の信号検出部16eとを備えている。

【0152】ホールセンサ16fは、コイルアンテナ20から磁気信号で送信される暗号元コードCRを受信して電気信号に変換し、信号検出部16eは、電気信号内の特定データを制御回路14に入力する。この場合も、コイルアンテナ20の代わりに永久磁石を用いることができ、車両コントロール装置30側の消費電力を節約し、コスト低減を実現することができる。

【0153】実施の形態5. また、上記実施の形態3および4では、暗号元コードCRを磁気信号で送信したが、光信号で送信してもよい。以下、暗号元コードCR

を光信号で送信するようにしたこの発明の実施の形態 4 を図について説明する。

【0154】図 10 はこの発明の実施の形態 5 による車両用リモコン装置 11 の構成を示すブロック図であり、図 10 において、受信回路 16 C は、受信部となる受光素子 16 g と、信号増幅部 16 h とを備えている。

【0155】受光素子 16 g は、車両コントロール装置 30 から赤外線などの光信号で送信される暗号元コード C R を受光し、データ内容を含む電気信号に変換して出力する。続いて、信号増幅部 16 h は、受光素子 16 g から出力される電気信号から暗号コードを取り出して制御回路 14 に入力する。

【0156】一方、車両コントロール装置 30 の送信回路 24 (図 1 参照) は、赤外線などの光信号を出力する発光装置 (図示せず) を含み、キーシリンダ 21 には、発光装置により駆動される発光素子 20 A が設けられている。発光素子 20 A は、キー 10 がキーシリンダ 21 に挿入されると、制御回路 25 の制御下で、光信号 (たとえば、赤外線) からなる暗号元コード C R を車両用リモコン装置 11 に送信する。

【0157】この場合、暗号元コード C R の送信手段として、コイルアンテナ 20 の代わりに発光素子 20 A が用いられるので、暗号元コード C R の送信時における車両コントロール装置 30 側の消費電力を節約することができる。

【0158】実施の形態 6. また、上記実施の形態 1 では、電波信号からなる暗号元コード C R を共振回路 16 a および 16 b を介して受信したが、高周波受信回路を介して受信してもよい。以下、車両用リモコン装置 11 内の受信回路として高周波受信回路を用いたこの発明の実施の形態 6 を図について説明する。

【0159】図 11 はこの発明の実施の形態 6 による車両用リモコン装置 11 の構成を示すブロック図であり、図 11 において、受信回路 16 D は、受信部となる R F 増幅部 16 i と、データ検出用の検波部 16 j と、検波用の周波数信号を出力する受信用発振部 16 k とを備えている。

【0160】R F 増幅部 16 i は、電波信号からなる暗号元コード C R を受信して増幅し、検波部 16 j に入力する。続いて、検波部 16 j は、受信用発振部 16 k からの発振周波数を用いて、増幅された受信信号から特定データ信号を検波して制御回路 14 に入力する。

【0161】図 11 においては、送信回路 15 が受信回路 16 D とは別に構成されているが、送信回路 15 は、受信回路 16 D とほぼ同構成の高周波送信回路により構成されているので、受信回路 16 D と共用に構成することができる。

【0162】すなわち、受信回路 16 D と同一の回路構成において、R F 増幅部 16 i から制御回路 14 に向かう受信信号に代えて、制御回路 14 から R F 増幅部に向

かう送信信号 (図示せず) を送信すればよい。

【0163】このように、単一の高周波送信回路で送受信回路を共用することにより、部品点数を削減してコストダウンを実現することができる。ただし、この場合、暗号元コード C R および暗号化コード C S の各送受信用周波数に整合させるため、制御回路 14 の制御下で、受信用発振部 16 k の出力信号の発振周波数を送受信毎に切り替える必要がある。

【0164】実施の形態 7. さらに、上記実施の形態 1 では、車両コントロール装置 30 が、手動スイッチ 12 の操作に基づく第 2 の暗号化コード C S 2 に応答してキーレスエントリ機能 (ドアロックの開閉制御) のみを実行するようにしたが、ドアロックの解除に続いて、自動的にイモビライザ機能 (エンジン始動許可) を実行するようにしてもよい。

【0165】すなわち、車両コントロール装置 30 は、第 2 の暗号化コード C S 2 が受信されたときに、自車両がドアロック状態であれば、第 2 の暗号化コード C S 2 がドアロック解除指令であると見なし、ドアロック制御信号 D L によりドアロックを解除するとともに、エンジンの始動許可信号 S T を生成する。

【0166】これにより、ユーザが車両に乗り込んでキー 10 をキーシリンダ 21 に挿入する前に、既にエンジン始動が可能な状態になっているので、エンジン始動の応答を迅速にすることができる。

【0167】なお、第 2 の暗号化コード C S 2 が受信されたときに、自車両がドアロック解除状態の場合には、第 2 の暗号化コード C S 2 がドアロック指令であると見なされるので、ドアロック制御信号 D L によりドアロックされるのみで、エンジンの始動許可信号 S T は生成されない。

【0168】

【発明の効果】以上のようにこの発明の請求項 1 によれば、車両のエンジン始動用のキーシリンダに挿入されるキーに内蔵され、且つ車両との間で相互に通信を行う車両用リモコン装置であって、キーシリンダへのキーの挿入時に車両側から送信される暗号元コードを受信する受信回路と、暗号元コードを記憶する記憶回路と、ユーザにより操作される手動スイッチと、暗号元コードの受信に応答して第 1 の暗号化コードを生成するとともに、手動スイッチの操作に応答して第 2 の暗号化コードを生成する制御回路と、第 1 および第 2 の暗号化コードを電波信号により車両側に送信する送信回路とを備え、第 1 の暗号化コードは、車両のエンジン始動を許可するための指令を含み、第 2 の暗号化コードは、記憶回路内の暗号元コードに基づいて生成され、車両のドアロックの施錠または開錠するための指令を含み、イモビライザ機能およびキーレスエントリ機能を統合してキー内に一体化するに、メンテナンス労力を低減した車両用リモコン装置が得られる効果がある。



【0169】また、この発明の請求項2によれば、請求項1において、暗号元コードは、車る。

【0170】また、この発明の請求項3によれば、請求項1において、制御回路は、記憶回向上させた車両用リモコン装置が得られる効果がある。

【0171】また、この発明の請求項4によれば、請求項1において、第1および第2の暗り機能を実現した車両用リモコン装置が得られる効果がある。

【0172】また、この発明の請求項5によれば、請求項1において、第1の暗号化コード果がある。

【0173】また、この発明の請求項6によれば、請求項1において、暗号元コードは、電コン装置が得られる効果がある。

【0174】また、この発明の請求項7によれば、請求項1において、暗号元コードは、磁費電力を軽減可能な車両用リモコン装置が得られる効果がある。

【0175】また、この発明の請求項8によれば、請求項1において、暗号元コードは、磁費電力を軽減可能な車両用リモコン装置が得られる効果がある。

【0176】また、この発明の請求項9によれば、請求項1において、暗号元コードは、光リモコン装置が得られる効果がある。

【0177】また、この発明の請求項10によれば、請求項1において、暗号元コードは、用構造により小形化が可能な車両用リモコン装置が得られる効果がある。

【0178】また、この発明の請求項11によれば、請求項1の車両用リモコン装置を用いインス労力の低減を実現した車両セキュリティ装置が得られる効果がある。

【0179】また、この発明の請求項12によれば、請求項11において、制御手段は、通果がある。

【0180】また、この発明の請求項13によれば、請求項12において、制御手段は、通得られる効果がある。

【0181】また、この発明の請求項14によれば、請求項11において、暗号元コードはた車両セキュリティ装置が得られる効果がある。

【0182】また、この発明の請求項15によれば、請求項14において、トリガ信号は、リティ装置が得られる効果がある。

【0183】また、この発明の請求項16によれば、請求項11において、車両コントロー向上させた車両セキュリティ装置が得られる効果がある。

【0184】また、この発明の請求項17によれば、請求項11において、車両用リモコンエントリ機能を達成可能な車両セキュリティ装置が得られる効果がある。

【0185】また、この発明の請求項18によれば、請求項11において、車両コントローセキュリティ装置が得られる効果がある。

【0186】また、この発明の請求項19によれば、請求項11において、車両コントロー信のための消費電力を軽減した車両セキュリティ装置が得られる効果がある。

【0187】また、この発明の請求項20によれば、請求項11において、車両コントローある。

【図面の簡単な説明】

【図1】 この発明の実施の形態1による車両セキュリティ装置を示すブロック構成図である。

【図2】 この発明の実施の形態1による車両用リモコン装置内の受信回路の構成例として電磁気作用を用いた場合を示すブロック図である。

【図3】 この発明の実施の形態1によるイモビライザ機能で用いられる暗号元コード内のトリガ信号の波形パターン例を示す説明図である。

【図4】 この発明の実施の形態1による車両用リモコン装置側の処理動作を示すフローチャートである。

【図5】 この発明の実施の形態1による車両コントロール装置側の処理動作を示すフローチャートである。

【図6】 この発明の実施の形態1によるイモビライザ機能でのデータ通信状態を時系列的に示す説明図である。

【図7】 この発明の実施の形態1によるキーレスエントリ機能でのデータ通信状態を時系列的に示す説明図である。

【図8】 この発明の実施の形態3による車両用リモコン装置内の受信回路の構成例（磁気抵抗素子を用いた場合）を示すブロック図である。

【図9】 この発明の実施の形態4による車両用リモコン装置内の受信回路の構成例（ホールセンサを用いた場合）を示すブロック図である。

【図10】 この発明の実施の形態5による車両用リモコン装置内の受信回路の構成例（受光素子を用いた場合）を示すブロック図である。

【図11】 この発明の実施の形態6による車両用リモコン装置内の受信回路の構成例（高周波受信回路を用いた場合）を示すブロック図である。

【図12】 従来のイモビライザ装置を示すブロック構成図である。

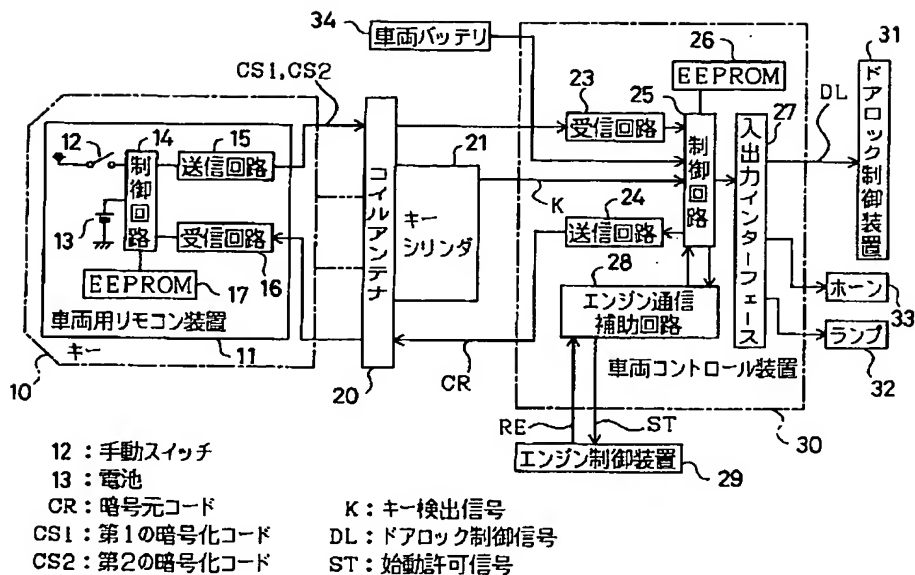
【図13】 従来のキーレスエントリ装置を示すブロック構成図である。

【符号の説明】

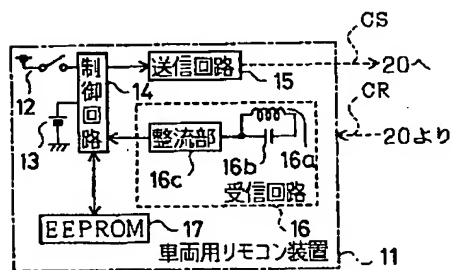
10 キー、11 車両用リモコン装置、12 手動スイッチ、13 電池、受信回路、16a コイル、16b コンデンサ、16d 磁気抵抗素子、16f ホールセンサ、16g 受光素子、16i RF増幅部、16j 検波判定するステップ、S70 ドアロック制御信号を出力するステップ。



【図1】

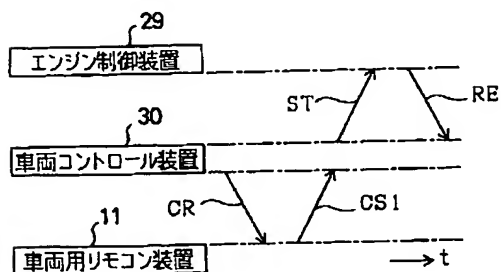


【図2】

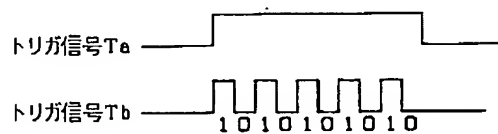


CS : 暗号化コード

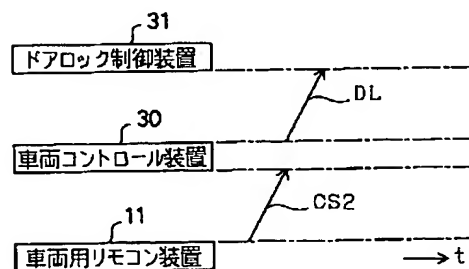
【図6】



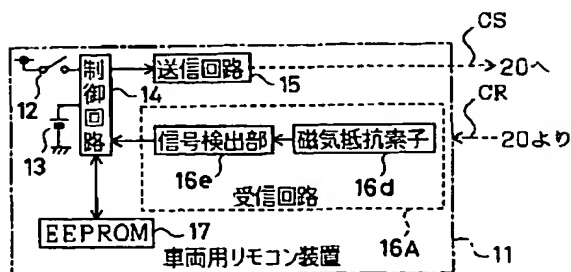
【図3】



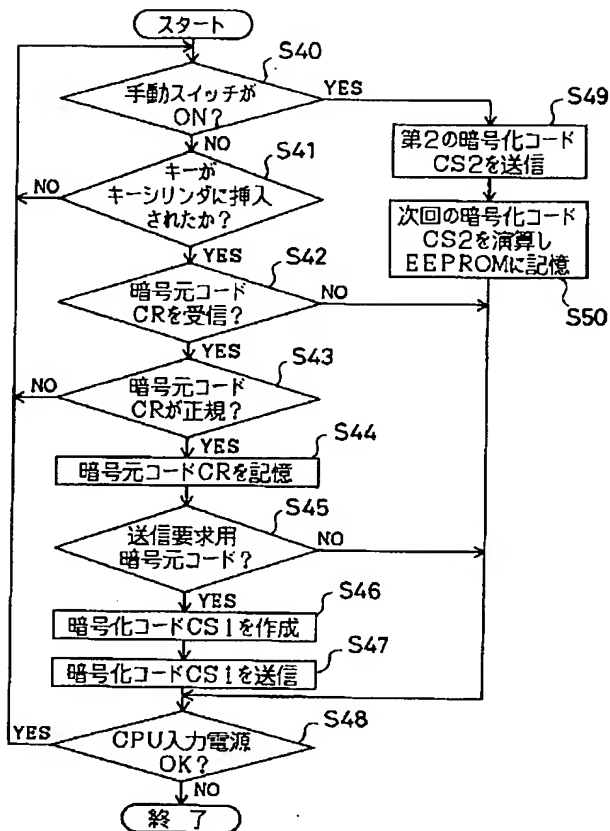
【図7】



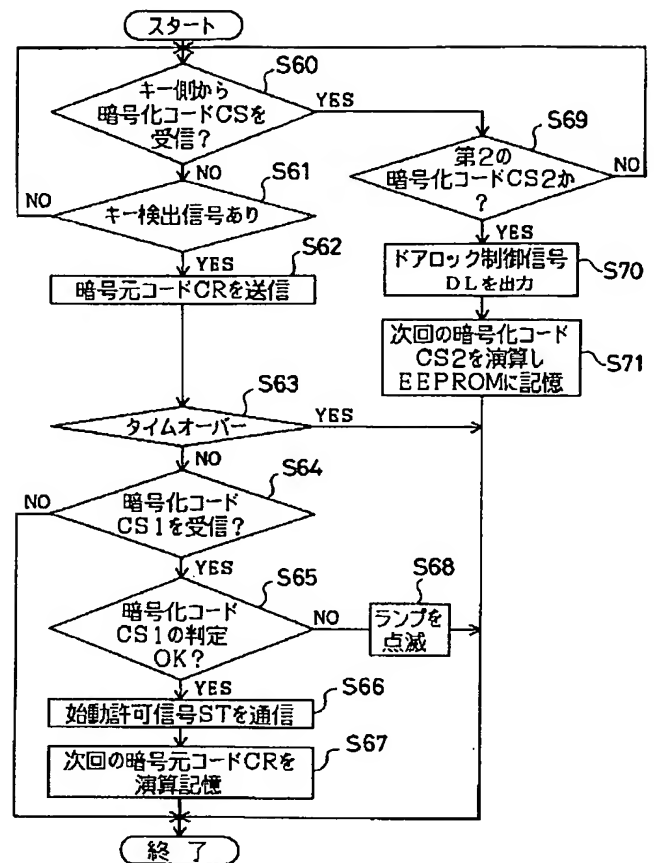
【図8】



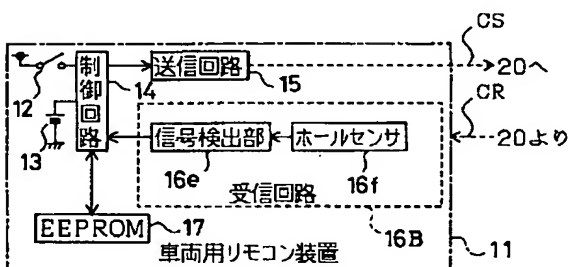
【図4】



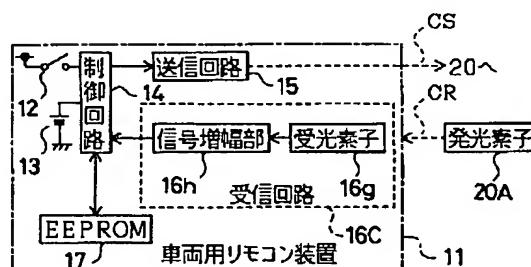
【図5】



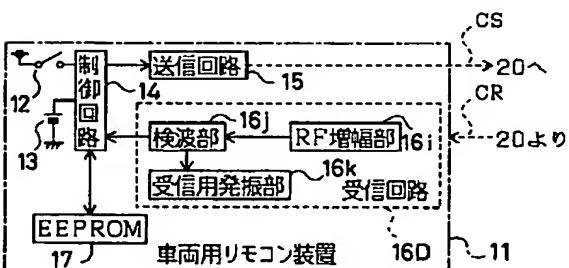
【図9】



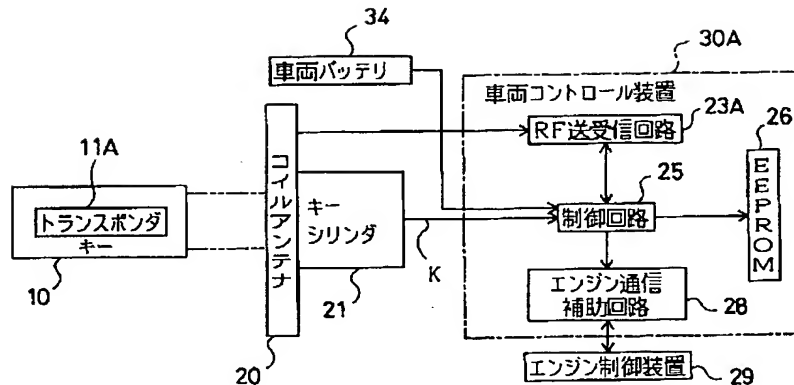
【図10】



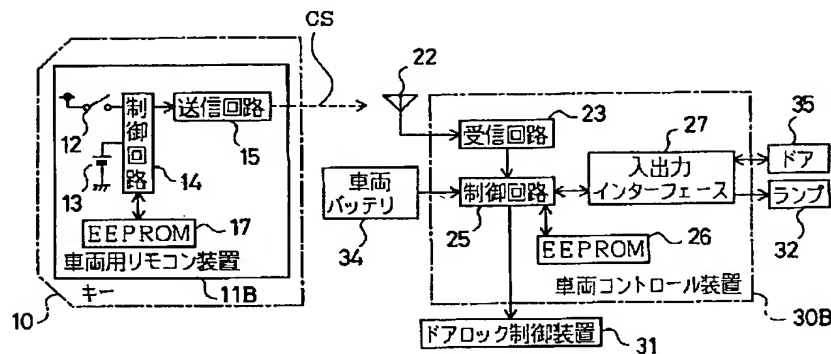
【図11】



【図12】



【図13】



## 【手続補正書】

【提出日】平成9年5月22日

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0169

【補正方法】変更

## 【補正内容】

【0169】また、この発明の請求項2によれば、請求項1において、暗号元コードは、車両を特定するために設定されたトリガ信号を含み、制御回路は、トリガ信号に基づいて暗号元コードの正規を判定するとともに、トリガ信号にตอบสนองして第1の暗号化コードを生成し、記憶回路は、正規と判定された暗号元コードのみを記憶するようにしたので、常に最新の暗号元コードを記憶し、要求が発生する毎に新規の暗号化コードを生成することのできる車両用リモコン装置が得られる効果がある。

## 【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0170

【補正方法】変更

## 【補正内容】

【0170】また、この発明の請求項3によれば、請求項1において、制御回路は、記憶回路に記憶された暗号元コードに基づいて、通信毎に異なる第2の暗号化コードを生成するようにしたので、他のキーに対して解読困難となり、セキュリティ度を向上させた車両用リモコン装置が得られる効果がある。

## 【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0171

【補正方法】変更

## 【補正内容】

【0171】また、この発明の請求項4によれば、請求項1において、第1および第2の暗号化コードが互いに異なるので、確実なイモビライザ機能およびキーレスエントリ機能を実現した車両用リモコン装置が得られる効果がある。

## 【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0172

【補正方法】変更

【補正内容】

【0172】また、この発明の請求項5によれば、請求項1において、第1の暗号化コードの電波出力は、第2の暗号化コードの電波出力よりも小さく設定されているので、第1の暗号化コードの電波漏洩による盗聴を防止するとともに、車両用リモコン装置内の電池の消費電力を最小限に抑制した車両用リモコン装置が得られる効果がある。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0173

【補正方法】変更

【補正内容】

【0173】また、この発明の請求項6によれば、請求項1において、暗号元コードは、電波信号からなり、受信回路は、インダクタンスを有するコイルとキャパシタンスを有するコンデンサとからなる共振回路を含み、共振回路を介した電磁結合により暗号元コードを受信するようにしたので、受信用の電源を省略した車両用リモコン装置が得られる効果がある。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0174

【補正方法】変更

【補正内容】

【0174】また、この発明の請求項7によれば、請求項1において、暗号元コードは、磁気信号からなり、受信回路は、磁気抵抗素子を含み、磁気抵抗素子を介して暗号元コードを受信するようにしたので、暗号元コードの送信手段に磁石を用いて消費電力を軽減可能な車両用リモコン装置が得られる効果がある。

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0175

【補正方法】変更

【補正内容】

【0175】また、この発明の請求項8によれば、請求項1において、暗号元コードは、磁気信号からなり、受信回路は、ホールセンサを含み、ホールセンサを介して暗号元コードを受信するようにしたので、暗号元コードの送信手段に磁石を用いて消費電力を軽減可能な車両用リモコン装置が得られる効果がある。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0176

【補正方法】変更

【補正内容】

【0176】また、この発明の請求項9によれば、請求

項1において、暗号元コードは、光信号からなり、受信回路は、受光素子を含み、受光素子を介して暗号元コードを受信するようにしたので、暗号元コードの送信側の消費電力を軽減可能な車両用リモコン装置が得られる効果がある。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0177

【補正方法】変更

【補正内容】

【0177】また、この発明の請求項10によれば、請求項1において、暗号元コードは、電波信号からなり、受信回路は、高周波受信回路からなるので、送信回路との共用構造により小形化が可能な車両用リモコン装置が得られる効果がある。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0178

【補正方法】変更

【補正内容】

【0178】また、この発明の請求項11によれば、請求項1の車両用リモコン装置を用いた車両セキュリティ装置であって、車両用リモコン装置が内蔵されたキーと、車両に設けられて、キーの挿入時にキー検出信号を生成するキーシリンダと、車両に搭載されて、車両用リモコン装置との間で相互に通信を行う車両コントロール装置とを備え、車両コントロール装置は、車両用リモコン装置から送信される第1および第2の暗号化コードを受信する受信手段と、キー検出信号に応答して暗号元コードを生成するとともに、第1および第2の暗号化コードの受信に応答して車両のエンジンおよびドアを制御する制御手段と、暗号元コードを車両用リモコン装置に送信するための送信手段とを含み、制御手段は、第1の暗号化コードに応答して車両のエンジン始動を許可するとともに、第2の暗号化コードに応答して車両のドアロックを制御し、イモビライザ機能およびキーレスエントリ機能を統合して一体化した車両コントロール装置を用い、車両用リモコン装置と協動するようにしたので、材料コストの低減、組み付けコストの低減およびメンテナンス労力の低減を実現した車両セキュリティ装置が得られる効果がある。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0179

【補正方法】変更

【補正内容】

【0179】また、この発明の請求項12によれば、請求項11において、制御手段は、通信毎に異なる暗号元コードを生成し、他のキーに対して解読困難な毎回異なる暗号元コードを送信するようにしたので、送信データ

の盗聴解読コピーによる不正なエンジン始動および車両盗難などの被害を確実に防止し、暗号化コードの使用におけるセキュリティ度をさらに向上させた車両セキュリティ装置が得られる効果がある。

【手続補正 12】

【補正対象書類名】明細書

【補正対象項目名】0180

【補正方法】変更

【補正内容】

【0180】また、この発明の請求項13によれば、請求項12において、制御手段は、通信毎にランダムカウント値を用いて暗号元コードを生成するようにしたので、送信データの盗聴解読コピーなどをさらに確実に防止した車両セキュリティ装置が得られる効果がある。

【手続補正 13】

【補正対象書類名】明細書

【補正対象項目名】0181

【補正方法】変更

【補正内容】

【0181】また、この発明の請求項14によれば、請求項11において、暗号元コードは、第1の暗号化コードの送信要求を車両用リモコン装置に指令するためのトリガ信号を含み、車両用リモコン装置側から自動的に第1の暗号化コードを送信させるようにしたので、特別な操作を必要とすることなくイモビライザ機能を実現した車両セキュリティ装置が得られる効果がある。

【手続補正 14】

【補正対象書類名】明細書

【補正対象項目名】0182

【補正方法】変更

【補正内容】

【0182】また、この発明の請求項15によれば、請求項14において、トリガ信号は、車両を特定するために設定された複数のデータの組合わせからなり、自車両を確実に特定できるようにしたので、さらにセキュリティ度を向上させた車両セキュリティ装置が得られる効果がある。

【手続補正 15】

【補正対象書類名】明細書

【補正対象項目名】0183

【補正方法】変更

【補正内容】

【0183】また、この発明の請求項16によれば、請求項11において、車両コントロール装置内の制御手段は、第2の暗号化コードに応答して、車両のドアロックを制御するとともに、車両のエンジン始動を許可するようにしたので、始動応答性を向上させた車両セキュリティ装置が得られる効果がある。

【手続補正 16】

【補正対象書類名】明細書

【補正対象項目名】0184

【補正方法】変更

【補正内容】

【0184】また、この発明の請求項17によれば、請求項11において、車両用リモコン装置内の制御回路は、第2の暗号化コードを送信毎に変更し、車両コントロール装置内の制御手段は、第2の暗号化コードを受信毎に変更し、車両コントロール装置は、受信毎に変更される第2の暗号化コードを記憶する記憶手段を含み、制御手段は、受信された第2の暗号化コードと、記憶手段に記憶された第2の暗号化コードとの差が一定範囲以内のときに、受信された第2の暗号化コードを正規と判定し、正規と判定された第2の暗号化コードのみに応答して、車両のドアロックを制御するようにしたので、送受信状態が多少不完全であっても、キーレスエントリー機能を達成可能な車両セキュリティ装置が得られる効果がある。

【手続補正 17】

【補正対象書類名】明細書

【補正対象項目名】0185

【補正方法】変更

【補正内容】

【0185】また、この発明の請求項18によれば、請求項11において、車両コントロール装置内の送信手段と協動するようにキーシリンダに配設されたリング状のコイルアンテナを備え、車両用リモコン装置内の受信回路は、インダクタンスを有するコイルとキャパシタンスを有するコンデンサとからなる共振回路を含み、暗号元コードは、電波信号からなり、共振回路を介した電磁結合により、コイルアンテナから受信回路に送信されるようにしたので、受信用の電源を省略した車両セキュリティ装置が得られる効果がある。

【手続補正 18】

【補正対象書類名】明細書

【補正対象項目名】0186

【補正方法】変更

【補正内容】

【0186】また、この発明の請求項19によれば、請求項11において、車両コントロール装置内の送信手段と協動するようにキーシリンダに配設された磁石手段を備え、暗号元コードは、磁気信号からなり、磁気応答作用により磁石手段を介して車両用リモコン装置内の受信回路に送信されるようにしたので、暗号元コードの送信のための消費電力を軽減した車両セキュリティ装置が得られる効果がある。

【手続補正 19】

【補正対象書類名】明細書

【補正対象項目名】0187

【補正方法】変更

【補正内容】

【0187】また、この発明の請求項20によれば、請求項11において、車両コントロール装置内の送信手段と協動するようにキーシリンダに配設された発光素子を備え、車両用リモコン装置内の受信回路は、受光素子を含み、暗号元コードは、光信号からなり、受光素子を介して受信回路に送信されるようにしたので、暗号元コードの送信のための消費電力を軽減した車両セキュリティ装置が得られる効果がある。

【手続補正20】

【補正対象書類名】明細書

【補正対象項目名】符号の説明

【補正方法】変更

【補正内容】

【符号の説明】

10 キー、11 車両用リモコン装置、12 手動スイッチ、13 電池、14、25 制御回路、15、24 送信回路、16、16A～16D、23 受信回路、16a コイル、16b コンデンサ、16d 磁気抵抗素子、16f ホールセンサ、16g 受光素子、16i RF増幅部、16j 検波部、16k 受信用発振部、17、26 EEPROM（記憶回路）、20 コイルアンテナ、20A 発光素子、21 キーシリンダ、27 入出力インターフェース回路、29 エンジン制御装置、30 車両コントロール装置、31 ドアロ

ック制御装置、32 ランプ、CR 暗号元コード、CS 暗号化コード、CS1 第1の暗号化コード、CS2 第2の暗号化コード、DL ドアロック制御信号、K キー検出信号、ST 始動許可信号、Ta、Tb トリガ信号、S40 手動スイッチのオン操作を判定するステップ、S41 キーシリンダへのキー挿入を判定するステップ、S42 暗号元コードの受信を判定するステップ、S43 受信された暗号元コードの正規を判定するステップ、S44 受信された暗号元コードを記憶するステップ、S46 第1の暗号化コードを作成するステップ、S47 第1の暗号化コードを送信するステップ、S49 第2の暗号化コードを送信するステップ、S50、S71 変更された次の第2の暗号化コードを演算して記憶するステップ、S60 暗号化コードの受信を判定するステップ、S61 キー検出信号の発生を判定するステップ、S62 暗号元コードを送信するステップ、S64 第1の暗号化コードを受信するステップ、S65 第1の暗号化コードの正規を判定するステップ、S66 始動許可信号を通信するステップ、S67 変更された次の暗号元コードを演算して記憶するステップ、S69 受信された暗号化コードが第2の暗号化コードか否かを判定するステップ、S70 ドアロック制御信号を出力するステップ。

フロントページの続き

(51) Int. Cl. <sup>6</sup>

識別記号

H04L 9/32

H04Q 9/00

301

F I

H04Q 9/00

H04L 9/00

301B

675A